**Основные теоретические сведения**

Цель: Получение практических и теоретических навыков работы с honeypot, способами и методами сканирования сети.

**1 Nmap**

Существует несколько средств сканирования Nmap, широко применяемых в настоящее время. Рассмотрим некоторые из них.

**1.1 TCP Connect()**

Второй доступный метод сканирования - TCP Connect. Он заключается в том, что сканирующая машина пытается установить соединение со сканируемой. Успешный результат говорит о том, что порт открыт, неудачный — о том, что он закрыт или фильтруется. Это сканирование легко обнаруживается по огромному количеству записей в log-файле неудачных попыток установления соединения и ошибок исполнения этой операции. Понятно, что средства защиты с максимальным быстродействием заблокируют адрес, вызывающий ошибки.

nmap –sT 192.168.58.103

-v: увеличить уровень вербальности (задать дважды или более для увеличения эффекта)

**1.2 TCP-SYN**

Более совершенным методом сканирования является TCP SYN — так называемое «полуоткрытое сканирование». При вызове Nmap посылает SYN-пакет, как бы ради того, чтобы установить новое соединение. Если в ответе присутствуют флаги SYN или ACK, считается, что порт открыт. Флаг RST говорит об обратном. Если пришел ответ, говорящий о том, что порт открыт, nmap незамедлительно отправляет RSTпакет для сброса еще не установленного соединения. Сканирование осуществляется только при наличии прав суперпользователя (root).

nmap –sS 192.168.58.103

**1.3 Сканирования FIN, Xmas Tree и NULL**

Тем не менее, межсетевой экран или другие защитные средства могут ожидать приходящие SYN-пакеты. Из-за этого зачастую такой метод сканирования не дает результата. Поэтому существует еще целая группа возможных способов сканирования, альтернативных TCP SYN. Это FIN, Xmas Tree и NULLсканирования. Большинство операционных систем по умолчанию, согласно рекомендациям, должны ответить на такие пакеты, прибывшие на закрытые порты флагом RST. Важная деталь: ни одна операционная система семейства Windows никогда не ответит RST пакетом на пришедший FIN, XmasTree или NULL пакет. Используя этот факт даже при подобных, в общем-то, не особо детальных сканированиях можно предположить, как минимум семейство операционных систем.

nmap –sF 192.168.58.103

nmap –sX 192.168.58.103

nmap –sN 192.168.58.103

**1.4 Сканирование протоколов IP**

Метод заключается в том, что хосту передаются IP пакеты без заголовков для каждого протокола сканируемого хоста. Если получено сообщение, говорящее о недоступности протокола, то этот протокол не поддерживается хостом. В противном случае — поддерживается.

nmap –sO 192.168.58.103

**1.5 ACK-сканирование**

ACK сканирование заключается в передаче ACK пакетов на сканируемый порт. Если в ответ приходит RST пакет, порт классифицируется как не фильтруемый. Если нет ответа или пришел ответ в форме ICMP-сообщения о недоступности порта, порт считается фильтруемым. Этот метод никогда не покажет состояние порта «открыт».

nmap –sA 192.168.58.103

**1.6 TCP Window**

TCP Window — похоже на ACK сканирование, однако по значениям поля Initial Window TCP-пакета пришедшего в ответ, можно определить открытые порты.

nmap –sW 192.168.58.103

**1.7 RPC-сканирование**

RPC-сканирование используется для определения программы, обслуживающей порт и её версии, и заключается в «затоплении» NULL- пакетами оболочки SunRPC открытых TCP или UDP портов хоста.

nmap –sR 192.168.58.103

**1.8 Сканирование ОС**

И, наконец, последнее — сканирование, используемое для определения ОС на сканируемом хосте.

nmap –O 192.168.58.103

**2. Honeypot**

Honeypot («Ловушка») - ресурс, представляющий собой приманку для злоумышленников.

Фактически основная задача Honeypot — подвергнуться атаке или несанкционированному сканированию с целью изучения стратегии и методов сканирования и определения перечня средств, необходимых для предотвращения будущих атак. Суть работы Honeypot заключается в создании ловушек — образов систем, которые извне воспринимаются как полноценные машины с установленными на них операционными системами, а, следовательно, поддающиеся сканированию.

Использование Honeypot имеет практический и исследовательский смысл. Во-первых, если на сервере установлена хорошая система защиты, долгое время можно не замечать постоянных попыток сканирования — Honeypot укажет на их наличие. Во-вторых, серьезной проблемой специалистов по информационной безопасности является нехватка информации о методах и средствах, используемых злоумышленниками. Единственное, что позволяет получить информацию об этих средствах — испытание их действия на себе. И Honeypot является чуть ли не идеальным способом для этого, ведь в настоящее время этом точно известно: грамотно настроенный Honeypot практически невозможно распознать.

Следует отметить, что в условиях, в которых проводится лабораторная работа, придется отойти от реальной ситуации, когда хакеру неизвестно ничего о том, что из себя представляет сервер и не являются ли подключенные к нему машины всего лишь ловушками. Иными словами, нам будут известны ip-адреса сканируемых ловушек.

Для начала необходимо создать локальную сеть из двух машин. Рекомендуется использовать машины с установленными на них операционными системами Ubuntu Server. Далее необходимо разобраться непосредственно с ловушками.

Изображение выглядит как текст, Шрифт, снимок экрана, логотип

Контент, сгенерированный ИИ, может содержать ошибки.

На виртуальную машину «Hacker» необходимо установить Nmap (либо в случае с операционной системой с графической оболочкой - Zenmap) . На виртуальную машину «Server» установить и настроить Honeyd.

Для выполнения данной работы на виртуальных машинах уже установлен весь необходимый софт

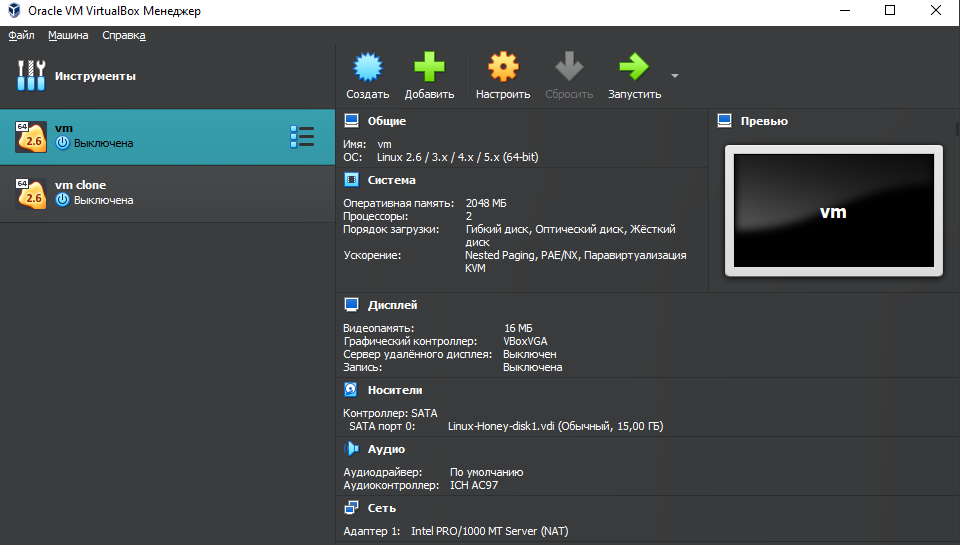
Практическая часть №1. Вариант 1.

Изображение выглядит как текст

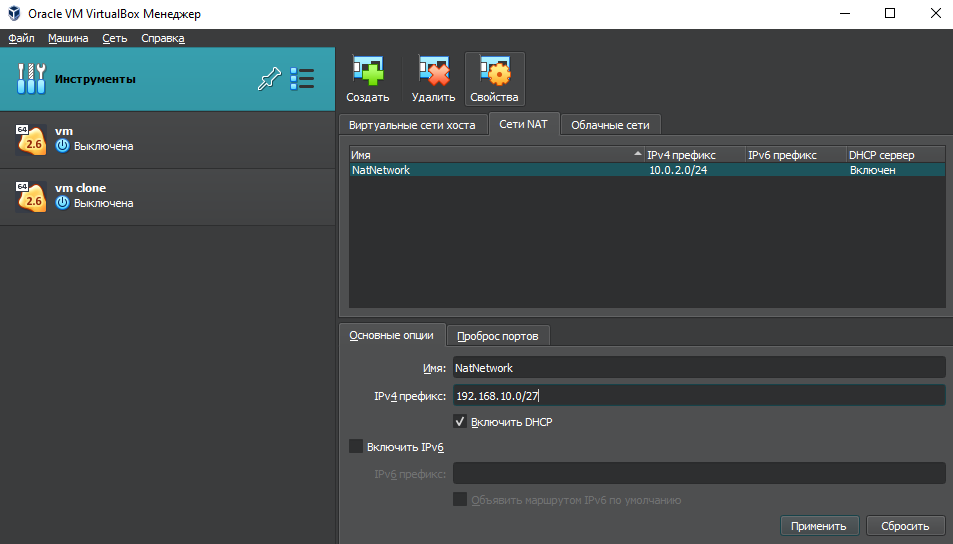
Автоматически созданное описание

Часть 1.

1. Создаём две виртуальные машины по готовому шаблону, данному в задании:



1. Создаём изолированную сеть “Nat” и задаём значение 192.168.10.0/27:



1. Подключаем обе виртуальные машины к “Nat” сети:

Изображение выглядит как текст, снимок экрана, монитор, экран

Автоматически созданное описание

1. Определяем IP адреса виртуальных машин используя команду “ip a”.

Первая машинa – 192.168.10.4/27:

Изображение выглядит как текст

Автоматически созданное описание

Вторая машина – 192.168.10.5/27:

Изображение выглядит как текст

Автоматически созданное описание

1. Измененяем конфигурационный файл “honeyd.conf” на первой машине согласно заданию:

Изображение выглядит как текст

Автоматически созданное описание

1. Открываем новый terminal и вводим “sudo farpd -d”:

Изображение выглядит как текст

Автоматически созданное описание

1. Запускаем на первой виртуальной машине honeyd с помощью команды “sudo -d -f /etc/honeypot/honeyd.conf ” в первой вкладке terminal и получаем в итоге:

Изображение выглядит как текст

Автоматически созданное описание

1. Производим сканирование нашей сети с honeypot всеми типами сканирования со второй машины:

1. TCP Connect ():

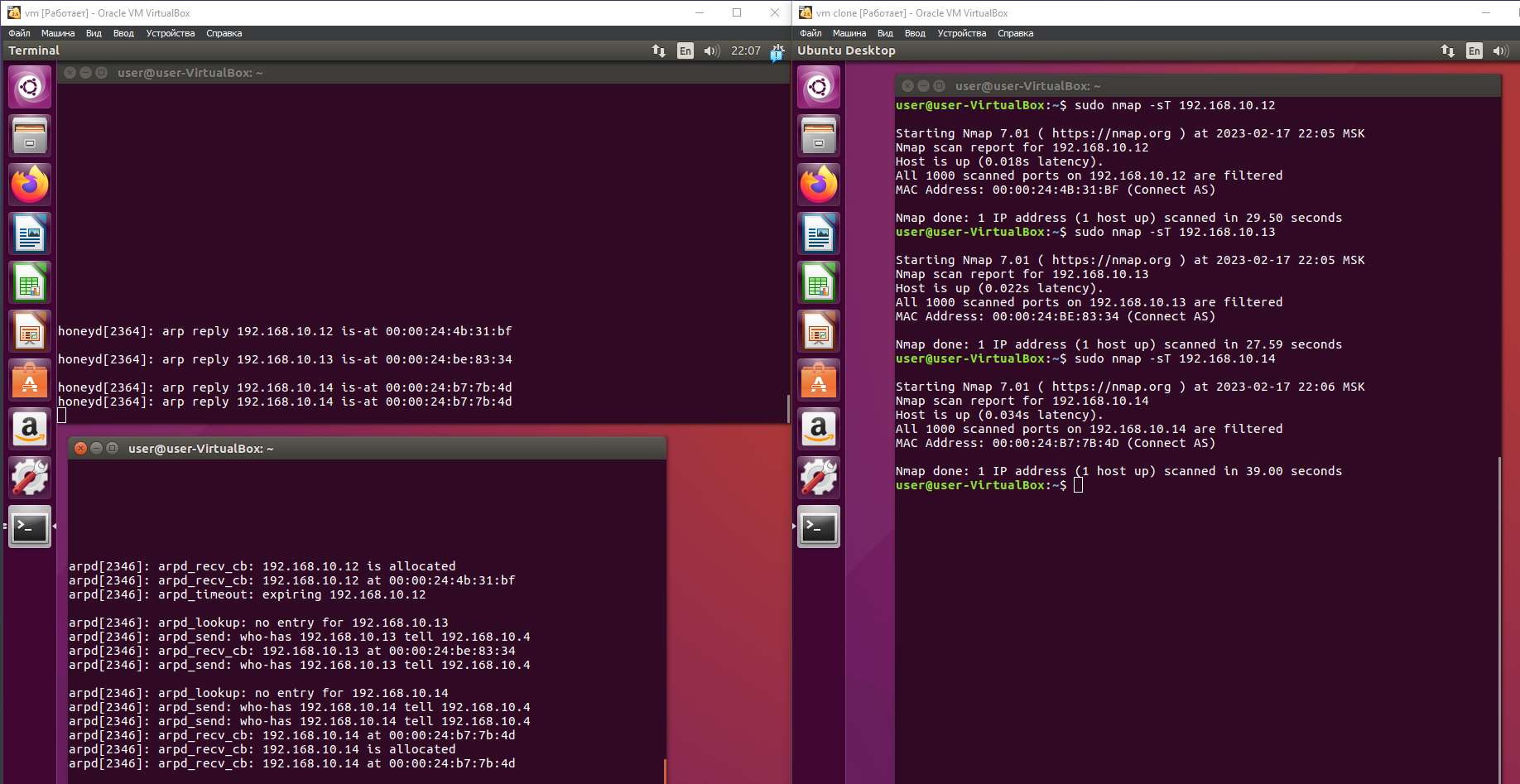
Вводим со второй машины последовательно команды:

sudo nmap –sT 192.168.10.12

sudo nmap –sT 192.168.10.13

sudo nmap –sT 192.168.10.14

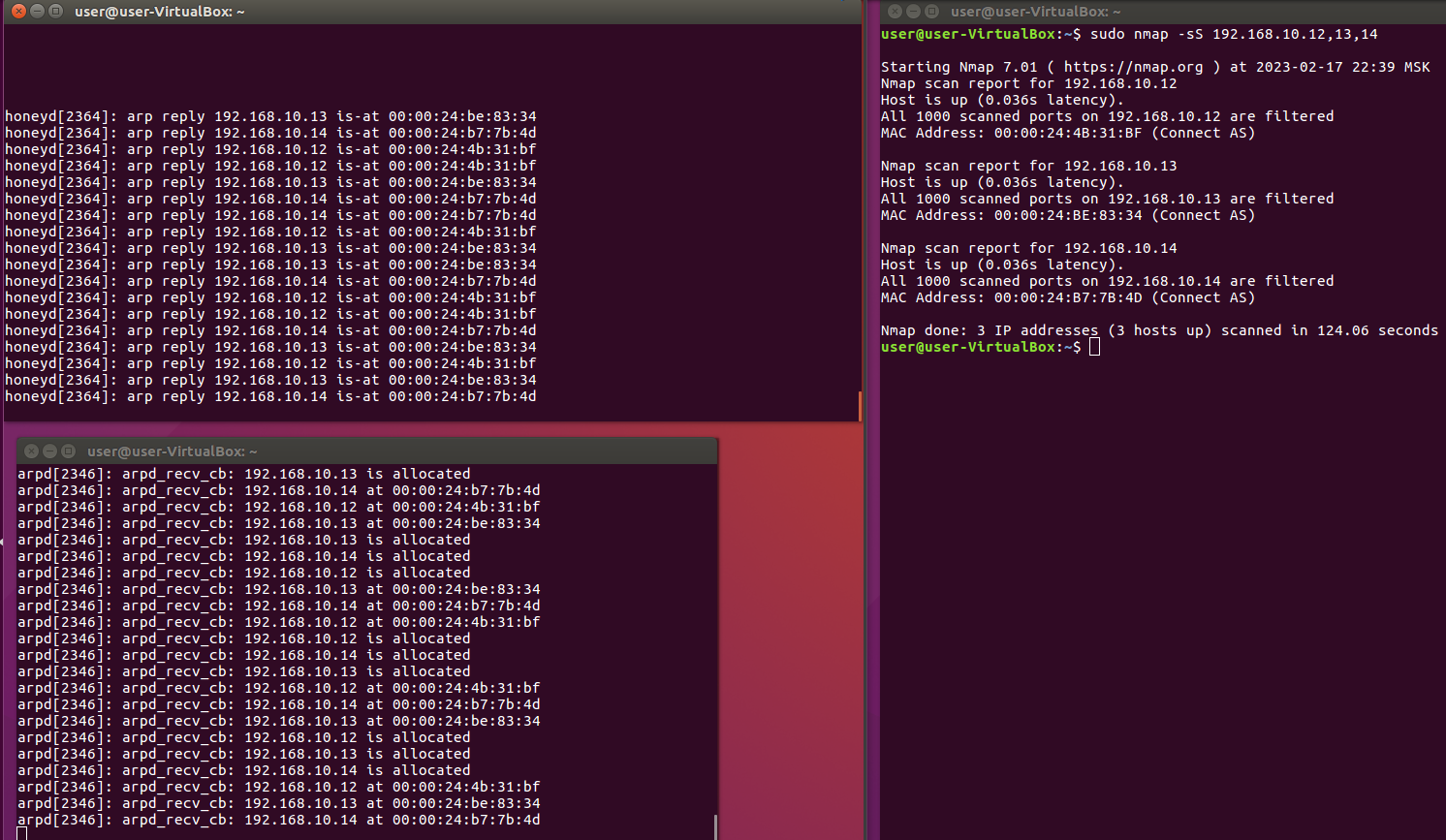
Получаем:



Видим, что данными командами nmap на второй виртуальной машине просканировал все ловушки, которые раннее были указаны в файле /etc/honeypot/honeyd.conf. Также заметим, что Honeyd указал на наличие попыток сканирования.

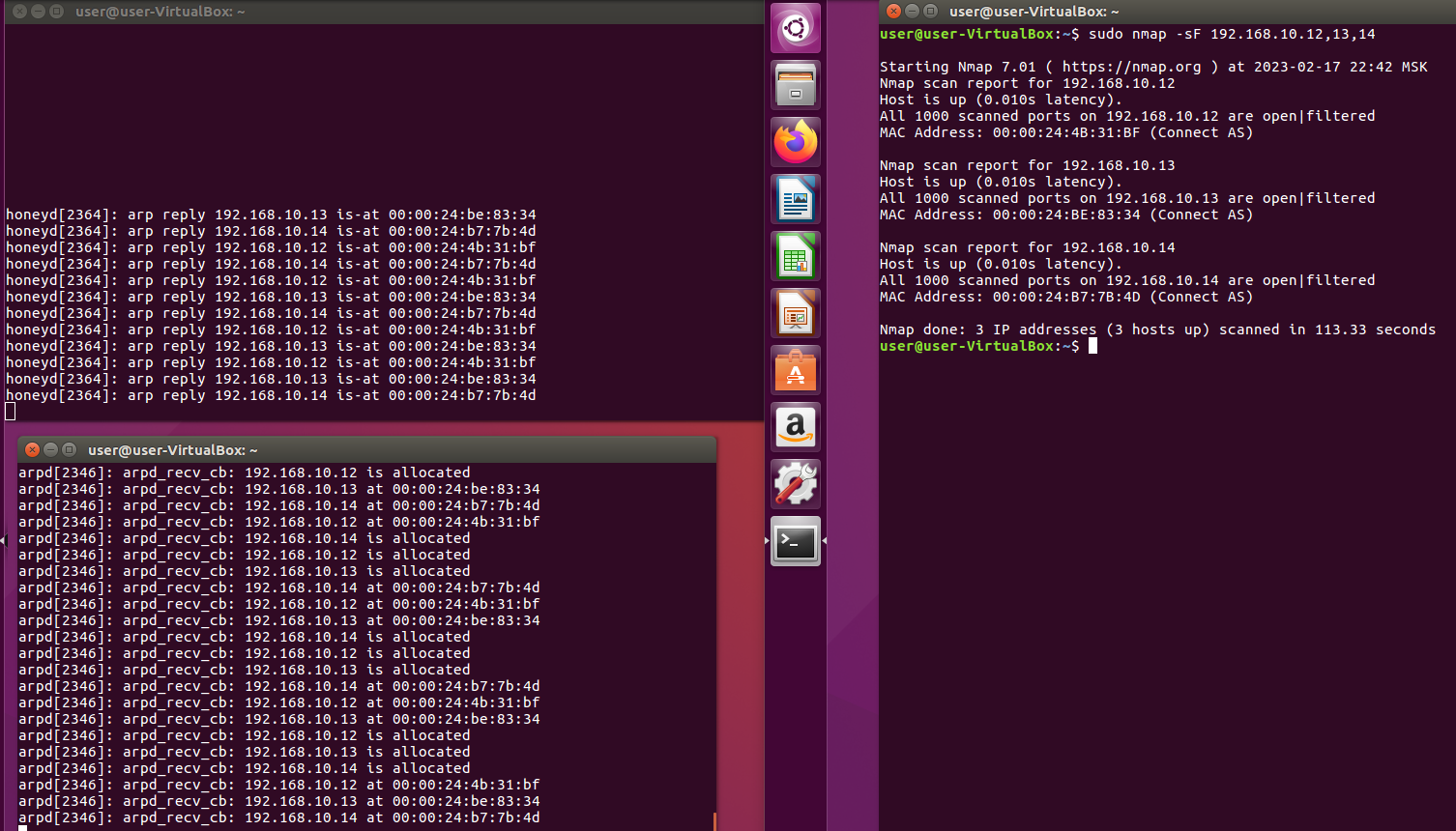
2. TCP-SYN полуоткрытое сканирование:

Вводим со второй машины команду “sudo nmap –sS 192.168.10.12,13,14” и получаем:



3. Сканирования FIN:

Вводим со второй машины команду “sudo nmap –sF 192.168.10.12,13,14” и получаем:



4. ACK-сканирование.

Вводим со второй машины команду “sudo nmap –sA 192.168.10.12,13,14” и получаем:

Изображение выглядит как текст

Автоматически созданное описание

5. Сканирование Xmas Tree:

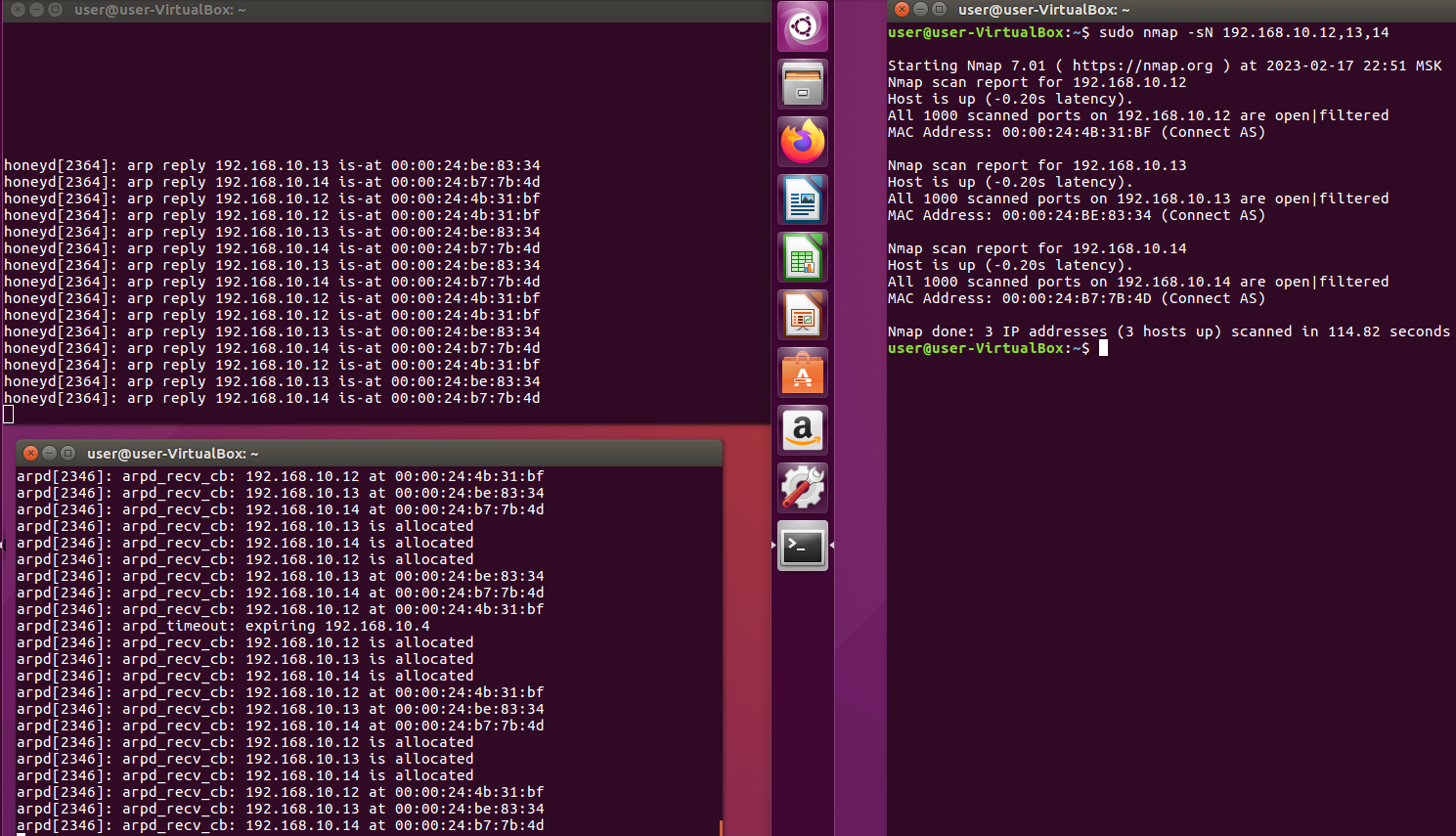
Вводим со второй машины команду “sudo nmap –sX 192.168.10.12,13,14” и получаем:

Изображение выглядит как текст

Автоматически созданное описание

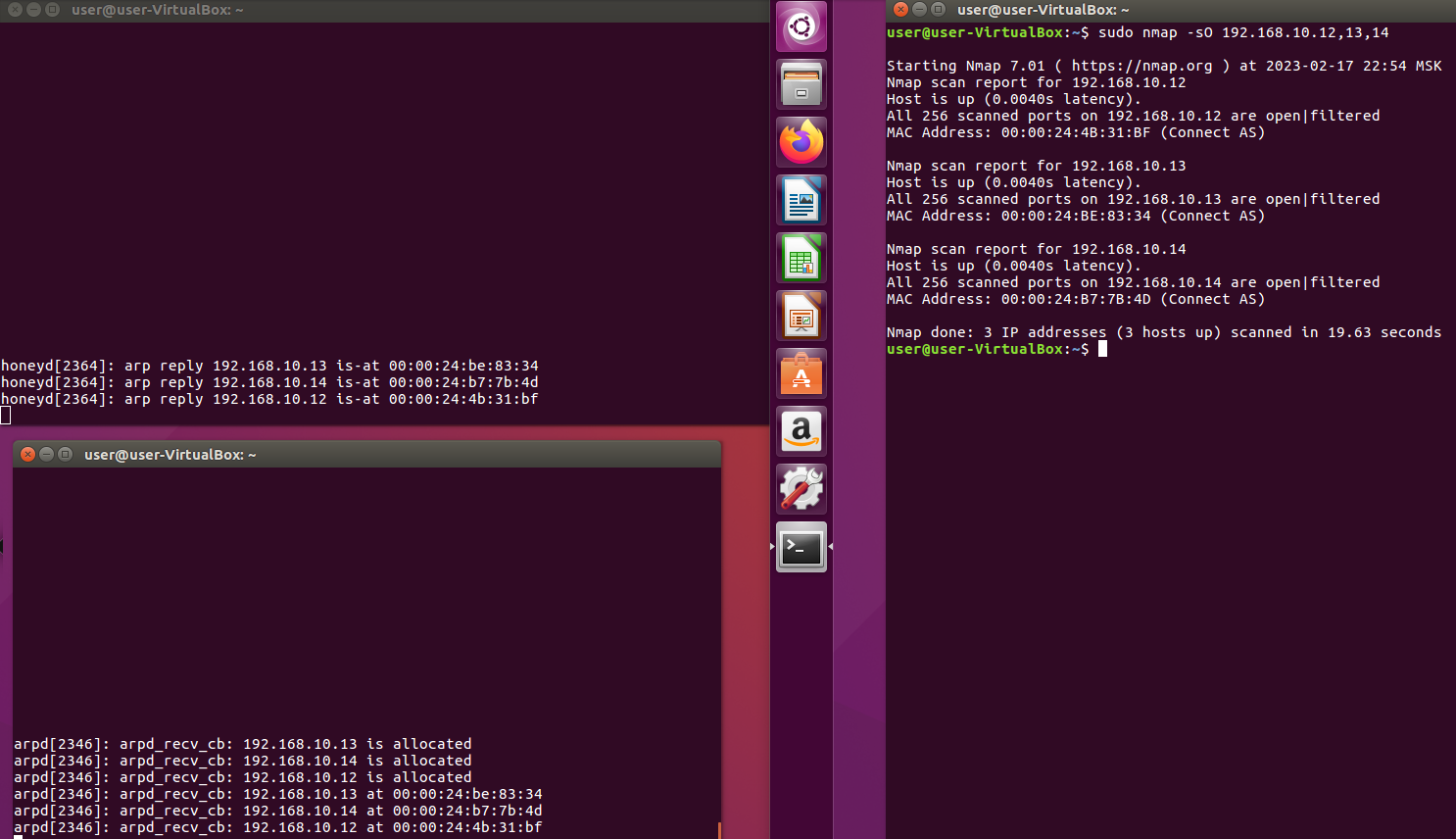
6. Сканирование NULL:

Вводим со второй машины команду “sudo nmap –sN 192.168.10.12,13,14” и получаем:



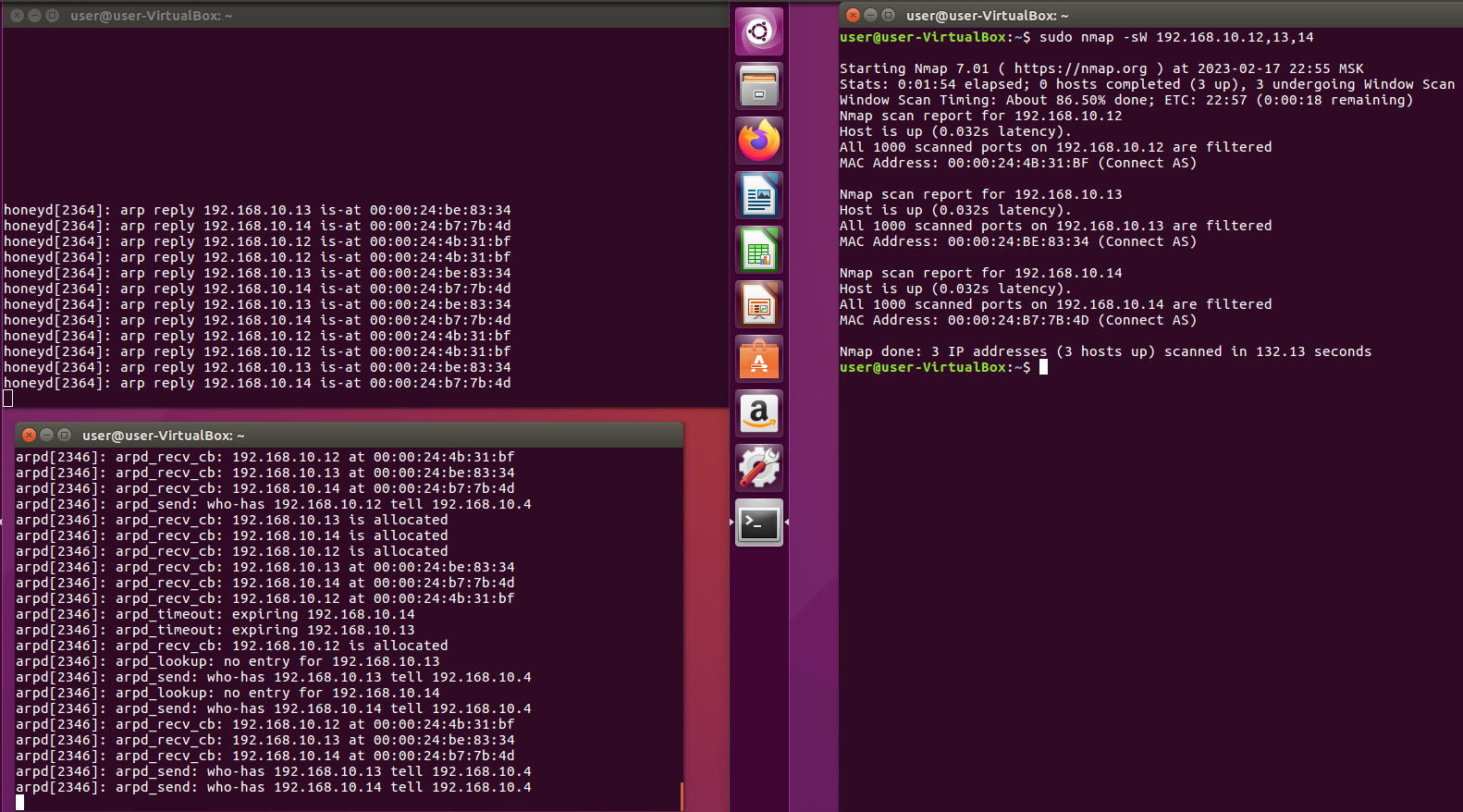
7. Сканирование протоколов IP:

Вводим со второй машины команду “sudo nmap –sO 192.168.10.12,13,14” и получаем:



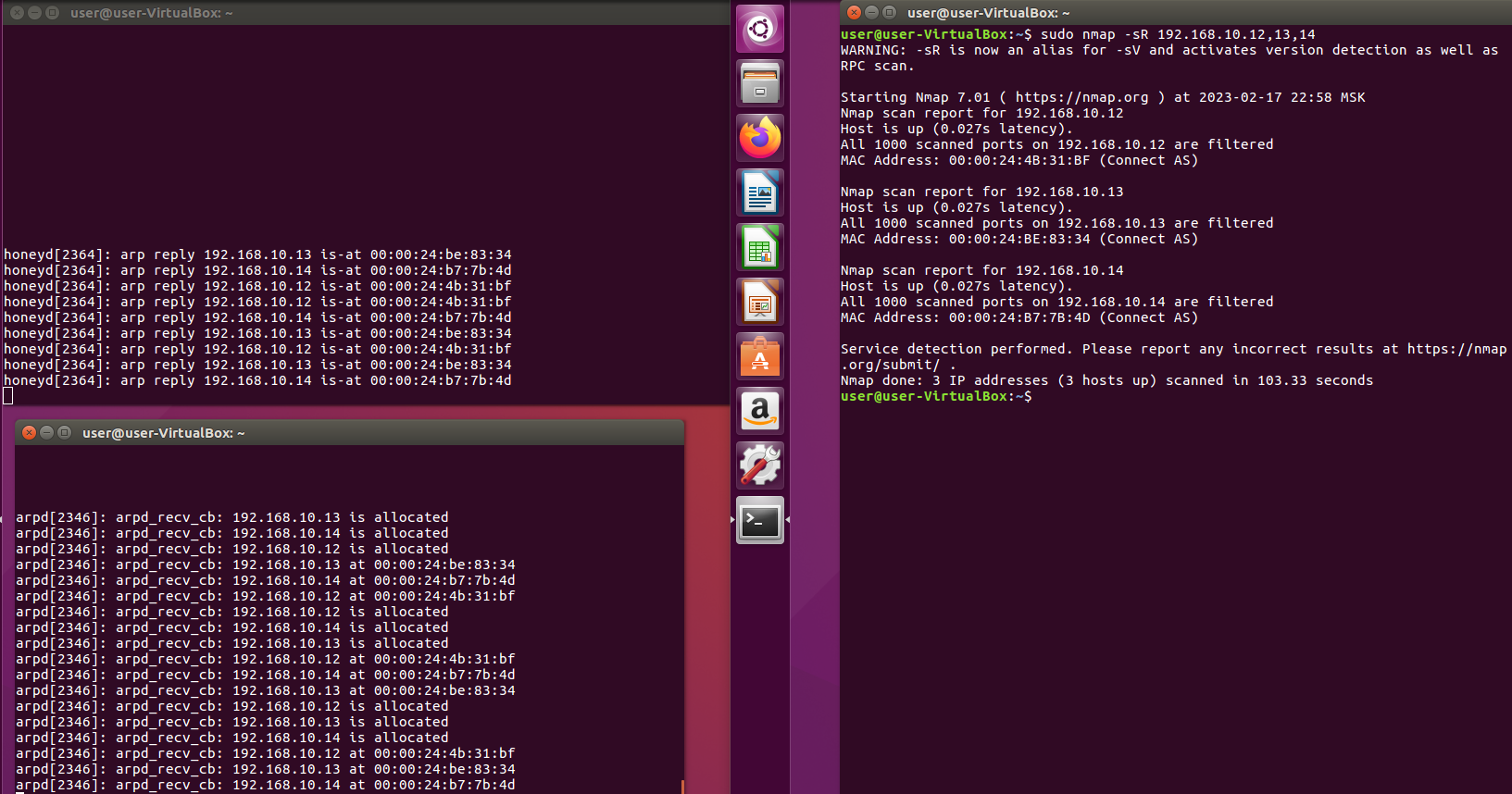
8. TCP Window:

Вводим со второй машины команду “sudo nmap –sW 192.168.10.12,13,14” и получаем:



9. RPC-сканирование:

Вводим со второй машины команду “sudo nmap –sR 192.168.10.12,13,14” и получаем:



10. Сканирование ОС:

Вводим со второй машины команду “sudo nmap –O 192.168.10.12,13,14” и получаем:



1. Изменяем настройки Honeypot на первой машине. Усложняем конфигурационный файл. Добавим template2 и template3 в качестве ещё одних ловушек.

Изображение выглядит как текст

Автоматически созданное описание

1. Запускаем honeyd с новыми настройками:

Изображение выглядит как текст

Автоматически созданное описание

1. Производим сканирование nmap. Воспользуемся командной “sudo nmap –sT 192.168.10.12,13,14,15,16”:

Изображение выглядит как текст

Автоматически созданное описание

Убеждаемся, что наши изменения конфигурации honeyd вошли в новое сканирование.

1. В результате всех сканирований, произведённых с помощью nmap, можно сделать вывод, что honeypot отлично справился со своей задачей “приманки”. Также отметим, что Honeyd исправно отобразил попытки сканирования.

Часть 2.

1. Убеждаемся в наличии интернет-соединения и запускаем анализатор трафика Wireshark.

Изображение выглядит как стол

Автоматически созданное описание

1. Проводим сканирование ip адреса 195.208.245.253 с помощью nmap:

Изображение выглядит как текст

Автоматически созданное описание

1. Отфильтруем пакеты, связанные с протоколом FTP:

Изображение выглядит как текст

Автоматически созданное описание

1. Анализируя перехваченные пакеты, можно предположить, что FTP сервер принадлежит Ростовскому государственному университету. Также в перехваченных пакетах можно заметить некоторые реплики, а также логин и пароль, которые использовались для сканирования FTP – сервера.
2. Логин и пароль можно заметить в столбце “info” в некоторых перехваченных пакетах. Логин – anonymous, пароль – IEUser@.

Ответы на вопросы к лабораторной работе:

Статический IP-адрес назначается конкретному устройству и при подключении к сети адрес не меняется. Чаще всего статические IP-адреса имеют веб-сайты.

Динамический IP-адрес позволяет изменять адрес устройства при каждом подключении к сети. Обычно динамический IP-адрес встречается у обычных пользователей.

Динамические адреса считаются более безопасными по сравнению со статическими, так как затрудняют отслеживание компьютера и других устройств, подключенных к сети.

1. Сканирование протоколов IP.

Метод заключается в том, что хосту передаются IP пакеты без заголовков для каждого протокола сканируемого хоста. Если получено сообщение, говорящее о недоступности протокола, то этот протокол не поддерживается хостом. В противном случае — поддерживается.

Большинство операционных систем по умолчанию, согласно рекомендациям, должны ответить на пакеты FIN, Xmas Tree и NULL сканирования, прибывшие на закрытые порты, флагом RST.

1. Honeypot

Honeypot («Ловушка») - ресурс, представляющий собой приманку для злоумышленников. Фактически основная задача Honeypot — подвергнуться атаке или несанкционированному сканированию с целью изучения стратегии и методов сканирования и определения перечня средств, необходимых для предотвращения будущих атак. Суть работы Honeypot заключается в создании ловушек — образов систем, которые извне воспринимаются как полноценные машины с установленными на них операционными системами, а, следовательно, поддающиеся сканированию.

1. Злоумышленники при проникновении в системы могут преследовать разные цели. Самые популярные цели:

1. Взлом сервера для скачивания каких-либо секретных данных, которые не должны быть доступны широкой общественности. Чаще всего такие взломы направляют против компаний для кражи отчетности, исходных кодов программ, секретной документации и так далее;

2. Изменение или уничтожение данных на сервере. Такие взломы могут производиться против любых серверов в сетях Интернет/Интранет. В качестве взломщиков могут выступать не только профессионалы, но и любители или даже недовольные сотрудники фирм;

3. Атака на сервер с целью сделать его недосягаемым для остальных участников сети. Этим занимаются в основном любители, желая нанести вред.

Серьезной проблемой специалистов по информационной безопасности является нехватка информации о методах и средствах, используемых злоумышленниками. Единственное, что позволяет получить информацию об этих средствах — испытание их действия на себе. И Honeypot является чуть ли не идеальным способом для этого, ведь в настоящее время этом точно известно: грамотно настроенный Honeypot практически невозможно распознать.

Однако в обратном случае, при плохо настроенном Honeypot, человек, сканирующий IP-адрес с помощью nmap может понять, что перед ним “ловушка”, если получит “подозрительный” результат сканирования.

1. Основные методы сканирования Nmap:

1. TCP Connect();

2. TCP-SYN – полуоткрытое сканирование;

3. Сканирования FIN;

4. Сканирования Xmas Tree;

5. Сканирования NULL;

6. ACK-сканирование;

7. Сканирование протоколов IP;

8. TCP Window;

9. RPC-сканирование;

10. Сканирование ОС.

Выводы:

В результате выполнения данной лабораторной работы были получены теоретические и практические навыки работы с honeypot, а также cо способами и методами сканирования.